report other than the "credit header" may reflect an individual's financial status, employment background, credit history, or medical records. The dissemination of this type of information is strictly regulated by the Fair Credit Reporting Act.[42]

Another possible proprietary or non-public source of identifying information for look-up services is marketing information. According to the Direct Marketing Association ("DMA"), which represents more than 3,000 United States corporations, information gathered for marketing purposes, *e.g.*, information gleaned from magazine subscription lists and warranty cards, should not be an information source for individual reference services.[43] The Commission, however, has learned of individual reference services that now offer, or offered until recently, data purportedly originating from marketing transactions.[44]

There are many other potential sources of non-public information. For example, some look-up services claim to obtain information from sources such as phone records, public utility records, and air travel records (indicating the airline, flight number, date, time, and even seat assignment for an individual's departure and return flight).[45] Other look-up services may obtain information elsewhere; however, because not all services reveal their sources for proprietary reasons, it is not possible to provide an exhaustive list.

C. Characteristics of Information Products

Individual reference services sell identifying information as raw data, in the form in which they received it, or they combine data from various sources and create enhanced information products or reports.[46] Accordingly, customers, upon entering search terms, can access information from one or more databases maintained by an individual reference service, or obtain gateway access into a database maintained by another entity.[47] The search may yield a compilation of identifying data used, for example, to locate an individual, or it may compare data entered by the customer to data in the database to verify an individual's identity.[48]

The scope of information offered by individual reference services varies significantly. Virtually all of these services include in their databases individuals' names and aliases, and current and prior addresses. Other services also make available certain unique identifiers, such as Social Security number, date of birth, and mother's maiden name.[49] Additional information may also include: place of birth, names and ages of family members and neighbors, schools attended, telephone numbers (listed and unlisted), employment information (past and present), physical characteristics, licenses held, voter registration information, driver's license number, automobile registration, personal identification numbers, association memberships, census information associated with the addresses, and asset ownership. Searches may also yield information about children, to the extent their identifying information is available.[50]

The number of databases employed by individual reference services to provide this information varies significantly as well. On one end of the spectrum, some look-up services provide access to one

database and display, for example, only current and prior addresses. On the other end, one service offered over the Internet claims to offer the following product:

> This is an amazing, revolutionary search. For one flat fee, this search takes any individual's name, or a company name, or any topic or subject, and runs it through 1,000 separate computer databases, which warehouse a collective 100 billion records. (Not million. Billion) Any and all information is returned that is found of [sic] the subject; length is unlimited. Many of the databases include Equifax, TRW, DBT, Trans Union, ABI, Dun & Bradstreet, IDS, CDB, Information America, DDI, TRW Business, Metromail, national newspaper database, national magazine database, UCCs, national lien and judgment search, national bankruptcy, national federal tax liens, national collection accounts, national mortgage search, national real property and many, many more. This combined search is truly remarkable. On searches conducted to date, the average report length has been 100 pages.[51]

Many information products fall somewhere between these extremes, yielding, for example, the results of searches of a series of public records databases relating to a particular topic, such as professional licenses or liens and judgments.

The cost to conduct a search ranges from roughly $1.50 to over $500.[52] The cost is a function of which reference service is offering the product (for example, an offline look-up service may charge $85 for a search that is available over the Internet for less than $10) as well as the depth, detail, and accuracy of the information sought.[53] Certain computerized databases offer identifying information to the public for free over the Internet.[54] The free services typically include access to one database containing public records maintained by government agencies or to white-page directories. Government agencies are increasingly making public records databases available for free over the Internet.[55] White-page directory databases are essentially computerized versions of white pages telephone directories and contain names, addresses, telephone numbers, and often E-mail addresses. Some of these look-up services allow "reverse" searches, enabling the user to enter the phone number or address and retrieve an individual's name.

D. Procedures Used to Restrict Access to Information

Offline commercial individual reference services have typically utilized proprietary networks (not the Internet) to transfer their information products to customers. Under this arrangement, customers may access the information via modem from a personal computer only after providing accurate and verified identifying and credit information,[56] entering into a subscription and payment agreement with the provider, and obtaining the necessary proprietary software.[57] Most individual reference services operating through their own proprietary networks do not offer their services to the public at large; instead they limit access to their services to what they deem to be legitimate businesses for legitimate purposes.[58] Some look-up services require a sign-up fee and monthly fees in addition to the per-search costs.[59] These costs may be high, further restricting the general public's access. Certain entities that sell information products in bulk to individual reference services impose similar access restrictions on their customers.[60]

The procedures used by the individual reference services to evaluate their customers and their contractual arrangements vary.[61] Some look-up services require new customers to complete an application in which the customer sets forth general purposes for accessing the information and agrees to use the information legally.[62] Other services may require a nexus between the user and the data subject.[63] Some services verify all the information in the application; others make sure that the applicant is a known business by conducting on-site visits[64] or by verifying that the phone number provided in the application matches the one listed in the telephone book under the business' name.[65] The level of scrutiny an applicant must undergo may also vary according to the type of information sought: certain look-up services grant access to public records, for example, with less stringent verification procedures,[66] or restrict access altogether to non-public sensitive information, such as Social Security numbers[67] and information about children.[68] In addition, look-up services may remind customers about permissible uses with messages that appear when the customer attempts to run particular searches.[69] A few services control risks of misuse by monitoring how their customers are using the databases and by maintaining audit trails of who has accessed which information.[70] Finally, look-up services may terminate or deny service for failure to abide by their procedures.[71]

As mentioned above, individual reference services have begun operating over the Internet.[72] Online services differ from offline services (*i.e.*, services that provide information through a proprietary network, but not over the Internet) in that they may be more readily accessible to a broader spectrum of customers. The range of information provided online parallels information provided through proprietary networks, and may be sold for less money.[73] One online service, for example, is reported to offer its subscribers an individual's Social Security number, birth date, and telephone number for just $1.50.[74]

Providing individual reference services over the Internet may pose unique problems with verification and access restrictions. In fact, several offline companies, acknowledging the risks in providing access to customers with whom they do not have an established business relationship, choose not to provide their non-public information services online.[75] Customers may attempt to access the services from computer terminals away from their home or office with Internet access accounts that shield their identity. Monitoring the uses by, and/or maintaining an audit trail of information accessed by, a user who successfully remains anonymous would probably not be very helpful in preventing or remedying misuse.

Certain online providers do take precautions to restrict access and prevent misuse. Some refuse to serve customers who are accessing their Web site anonymously,[76] and others require customers to enter into a subscription or use agreement,[77] as is the case with their offline counterparts. The majority of online white-page directory services limit the information they make available in the first place by: providing only information that is accessible from telephone companies, suppressing unlisted directory information, permitting consumers to opt out of having their information made publicly available, and not allowing reverse searches.[78] However, the barriers to entry for setting up a service online are remarkably low; by paying a local Internet service provider as little as $19.95 per month and purchasing information from a vendor, anyone can publish a Web site with whatever information she chooses.[79] Thus, it is possible that some companies providing services online may offer information more widely, with fewer restrictions.

III

Beneficial Uses

Individual reference services cater to a wide array of customers, from law enforcement agents and corporations to public interest groups and individual consumers. Users agree that, although the same information may be available from other sources, having access to computerized databases enables them to obtain the information, and therefore conduct searches and investigations, much more quickly.[80] Additionally, some point out that increased accessibility to more information is necessary because people are becoming more mobile and, accordingly, more difficult to find.[81]

A. Public Sector Uses

Individual reference services provide critical assistance to federal, state, and local government agencies to carry out their law enforcement and other missions.[82] Agencies, including the Federal Trade Commission, rely on the databases to detect perpetrators of fraud, to locate and identify suspects and related businesses, and to track down witnesses.[83] Agencies emphasize the importance of having access to all possible identifying information.[84] A subject's prior addresses may point to locations where other law enforcement agencies may have warrants or case information.[85] Knowing the identities of suspects' neighbors is sometimes necessary for their protection.[86] UCC filings, and lien and judgment records can link individuals and companies.[87]

Computerized databases play a particularly useful role in the prosecution of financial crimes. The Financial Crimes Enforcement Network, an arm of the US Department of the Treasury, (hereinafter "FinCEN") relies heavily on computerized databases to prevent and detect money laundering.[88] FinCEN carries out this mission in part by combining information it receives from banks and other financial institutions with government and public information.[89] It then discloses the information to other law enforcement agencies in the form of intelligence reports.[90] FinCEN also grants law enforcement officials in each state online access to its financial database.[91] Because so many law enforcement agencies rely on FinCEN for analytical support, FinCEN is even able to connect agencies that are investigating the same crime or individual.[92] The National White Collar Crime Center, a non-profit organization funded by the US Justice Department, also subscribes to individual reference services and, like FinCEN, conducts searches on behalf of member agencies with criminal investigative authority related to economic crimes.[93] In addition, the US Secret Service subscribes to approximately thirteen of these databases. The Secret Service uses them to fulfill its mission to investigate counterfeit currency and financial crimes, by locating targets and detecting fraudulent practices, as well as its mission to protect public officials, by locating individuals who pose a threat or who have information regarding potential threats.

B. Private Sector Uses

Individual reference services provide myriad benefits to the private sector as well.[94] The services play important roles for diverse entities, including insurance companies, banks, creditors, retailers, lawyers, private investigators, non-profit agencies, and journalists. Private sector representatives emphasize that many of their purposes for using these services, like fraud prevention and the enforcement of court orders, overlap with those of law enforcement.[95] In light of the increasing case loads and decreasing budgets of many law enforcement agencies, they note that private sector contributions in these areas are critical.[96]

The corporate sector appears to employ the look-up services primarily to detect and investigate potential fraud. The insurance industry, for example, relies on these services to investigate fraudulent claims.[97] Many people who submit fraudulent insurance claims use a fake name or Social Security number; insurance companies can detect these cases by verifying the claimant's personal identifying information through a service.[98] Credit grantors in the retail and other industries use information provided by the look-up services to confirm the identity of credit applicants.[99] They, too, make sure that all of the identifying information provided by the applicant matches the information retrieved through the services, in order to detect and limit potential fraud.[100] Banks have affirmative obligations to report credit card fraud, insider abuse, and money laundering.[101] To fulfill these obligations, they use the look-up services to: verify the validity of identifying information, such as Social Security numbers, provided by new account applicants;[102] implement required "know your customer" policies;[103] and ensure that potential employees have clean records.[104] Many businesses also subscribe to look-up services to conduct due diligence investigations[105] to minimize the risk of financial fraud in business dealings, and to locate business debtors.[106] Private organizations may also use look-up services in connection with fund-raising efforts.

In relying on look-up services to prevent fraud in connection with credit and job applications, the corporate sector may be using information provided by look-up services to make decisions about whether to grant consumers credit or jobs.[107] The precise information these entities are using to make such decisions remains unclear.[108] To the extent that entities are making credit, insurance, or employment decisions about individuals based on information in consumer reports (*e.g.*, credit history, financial status, and employment background information), their uses would be subject to certain obligations and restrictions set forth in the Fair Credit Reporting Act.[109]

The legal profession, either directly or through third parties like private investigators, relies on individual reference services for many purposes, including locating witnesses;[110] identifying parties and witnesses with a financial stake in the outcome of cases;[111] finding assets to satisfy judgments;[112] conducting due diligence investigations of financial representations;[113] and locating debtors, heirs, and pension fund beneficiaries.[114] In addition, private investigators use look-up services when hired by businesses to prevent or detect insurance fraud, bank fraud, and identity theft.[115] Finally, they use look-up services on behalf of consumers to reunite families; to locate missing or abducted persons; to carry out prenuptial investigations; to stop stalkers; or to track down non-custodial parents who owe child support.[116]

Many public-interest oriented organizations rely on individual reference services for quasi-law enforcement purposes, such as detecting fraud in connection with campaign financing, finding missing children, curbing domestic violence, and enforcing child support orders.[117] Government watchdog groups and others rely on individual reference services to access Federal Election Commission filings to monitor

the records of federal campaign contributions.[118] Agencies such as the Center for Missing and Exploited Children track down abducted children and run-away teens by combining data such as name, address, Social Security number, and school enrollment lists obtained from both private and public databases.[119] Other groups use look-up services to prevent child and elder exploitation in the first place, by conducting background checks of potential care providers.[120] Health care organizations use the look-up services to locate organ and bone marrow donors.[121] The services are also instrumental in assisting organizations find non-custodial parents who have neglected to pay court-ordered child support.[122] The parents can then provide this information to their government child-support agency or use it to initiate their own court action.[123] These organizations also emphasize the need to have access to as much identifying information as possible. For example, one non-profit agency claims a 90 percent success rate in finding parents who owe child support when provided with a Social Security number, compared to a 57 percent success rate without it.[124]

Individual reference services play an important role in journalism as well. Journalists use the services to ensure the accuracy of their stories, for example, by independently verifying the identity of a news subject.[125] The look-up services also enable reporters to enhance their stories with background information on news subjects, like disaster victims and elected officials.[126] Journalists also emphasize the value of having access to as much identifying information as possible.[127]

C. Consumer Uses

Many of the uses outlined above ultimately benefit consumers. Look-up services that serve consumers, not just businesses, enable individuals to find information for any of the uses outlined in this section, without having to hire an intermediary to do it for them. By using these look-up services (typically offered over the Internet), consumers can independently locate an old friend or family member, verify land title in the course of a real estate transaction, or verify the validity of licenses of medical or other professionals.[128] Furthermore, consumers indirectly benefit from this industry in that fraud prevention in the corporate sector helps to keep consumer prices down.[129] Moreover, society as a whole may benefit to the extent that this industry enables the media to more timely and accurately report the news.

IV
Risks

While the individual reference services industry bestows undeniable benefits on society, the wide availability of personal information also poses risks to consumers' psychological, financial, and physical well-being. Consumers may be adversely affected by a perceived privacy invasion, the misuse of accurate information, or the reliance on inaccurate information. A meaningful risk assessment begins with an acknowledgment that because consumers are not the customers of these companies,[130] the companies have little marketplace pressure to respond to consumer interests. Furthermore, because consumers do not have a direct relationship with look-up services, they may remain unaware of possible exposure to risks.[131] Finally, consumers have few means to protect themselves.[132]

A. Impact on Consumers' Privacy Interests

Survey research over the past 20 years demonstrates that increasing numbers of Americans are concerned about how personal information is being used in the Computer Age.[133] A recent poll indicates that a sizeable majority of Americans -- 88 percent -- are concerned particularly about the sale of their Social Security numbers and other personal identifiers.[134]

With increasing attention to privacy by the press, consumers are only now beginning to learn about the individual reference services industry.[135] The outrage many consumers expressed last year in response to learning about the availability of their Social Security numbers through LEXIS-NEXIS' P-Trak service suggests that they would be even more concerned to learn about the wide availability of sensitive information through other services.[136] Once consumers disclose their information to private entities, or once it is transferred from a public records custodian, where data subjects at least have the possibility of seeing and correcting their own records, consumers essentially lose their ability to access information maintained about them.[137] As data subjects have no relationship with companies offering individual reference services, they have few means to determine which organizations store and communicate information about them to others.[138] Furthermore, given this lack of privity, consumers as data subjects do not necessarily derive a direct benefit from the service.[139] Even if consumers were able to determine who was storing and selling information about them, only in rare instances could they access records containing data about them, correct any errors, find out who has accessed their records, or have their records removed from private databases.[140]

Consumers' concerns about the privacy of their personal information are closely related to the sensitivity, both real and perceived, of that information. The perceived sensitivity of information varies

with each individual and with the context in which the information is requested or made available.[141] Many people, for example, are completely comfortable listing their home address in the white pages, while others may take precautions not to disclose this information unless absolutely necessary.[142] Furthermore, while individuals may not be concerned with certain pieces of information when standing alone, they may perceive those same pieces of information as sensitive when integrated together,[143] or when used to uncover more potentially sensitive information (such as using name and birth date to obtain Social Security number).[144] Individuals also may change their idea of what is sensitive as they discover that others are accessing their information for business or other purposes inconsistent with the purpose for which it was originally furnished.[145] For example, an individual may be comfortable providing income information when applying for a loan or a parent may willingly disclose a child's age to register the child in school, but would not want this information made publicly available.[146] Furthermore, many consumers feel comfortable with others being able to discover their phone number or address using their name as a search term, but do not feel comfortable when their phone number or address is used to find out their name through a "reverse search."[147] Moreover, comfort with the availability of information in the physical world may not transfer to comfort with the availability of the same information over the Internet.[148] Finally, the same piece of information (*e.g.*, age) may raise different privacy concerns at different points in a person's life.[149]

Certain unique identifiers, like Social Security number, are more uniformly perceived as sensitive. This perception is reflected in recent survey findings as well as by the public's response to learning that their Social Security numbers were available through LEXIS-NEXIS' P-Trak service.[150] This sensitivity is understandable given that many entities use Social Security numbers to identify an individual before either granting access to more information, like a bank account balance, or conferring a benefit, like opening a credit card account.[151] Date of birth[152] and mother's maiden name may be considered sensitive for this same reason.[153]

Surveys conducted regarding consumers' opinions about public records information further illustrate that sensitivity is generally a function of both content and context. Although consumers readily provide their information to government agencies for discrete purposes (or when compelled to do so), they do not support the government making all public records readily available. For example, one survey has found that 92 percent of American adults believe it is at least somewhat important that state agencies not be able to sell or release personal data about them without their knowledge or consent.[154] Similarly, another study concluded that 75 percent of American computer users object to the wide availability of public records via the Internet.[155] A third survey asked consumers how they felt about businesses accessing certain public records to prevent insurance fraud.[156] The survey found that 60 percent of Americans support the use of criminal records to combat insurance fraud and 51 percent support the use of motor vehicle records for that purpose.[157] This support wanes, however, for the use of worker's compensation records (40 percent), health claims data (36 percent), medical records (31 percent), or pharmaceutical data (25 percent) to combat insurance fraud.[158]

B. Risks Associated With Inaccurate Data

It is not difficult to imagine how inaccurate information products could bring real harm to consumers. A doctor whose professional license records are mistakenly excluded from a professional licenses database may have a tough time recruiting new patients. An entrepreneur whose records are crossed with those of a convicted white collar criminal with the same name may not find many willing business partners. Similarly, an operator of a day-care center whose identifying information, because of a typographical error,

indicates that a previous address is that of a local strip bar may not stay in business very long.[159] The record reflects that, in an effort to prevent fraud, certain entities use information obtained through the look-up services to decide whether to grant an individual a job or credit.[160] If the information offered by the applicant does not match the information obtained through the look-up services, the applicant may be denied credit or employment. Inaccurate information in the look-up services could cause an honest individual to be denied credit or employment wrongfully. Finally, inaccurate information obtained through a look-up service could result in an individual not being found and therefore not receiving an earned benefit (*e.g.*, pension benefits) or suffering harm (*e.g.*, not learning of prior exposure to toxic chemicals)

Given the ease with which information can be gathered, aggregated, and shared, errors could be widely replicated[161] and the harm long-lasting. As described by one industry representative, the information obtained through individual reference services is unverified data, entered initially by human beings and accordingly subject to human error.[162] While some companies warn their customers of this up-front,[163] others tout the accuracy of their information products. One large supplier of public records information assures its customers that the information it sells is at least 99 percent accurate.[164] An information industry association states that because these databases aggregate information from several sources, the information products tend to be more accurate.[165] Several industry representatives point out that the information must be accurate because the market demands accuracy.[166]

Even at their source, however, records may contain typographical errors, misspellings, or omissions.[167] Furthermore, once records are transferred to secondary information providers, they may not reflect the most current information (depending on the method of data collection or backlog in updating the records at their source).[168] They may contain errors caused during the creation of public records indices[169] or during the transcription or transmission of the original records. Moreover, due to overlap in identifying information, the results of a search of records compiled from several sources could reflect a mismatch, displaying accurate information about someone, but not necessarily the targeted individual.[170]

Data subjects generally do not have the ability to access the data maintained about them by individual reference services to correct errors.[171] Consumers may in some cases succeed in obtaining a copy of their records only by hiring a professional to buy the relevant information products from look-up services to which the professional subscribes.[172] Alternatively, consumers could buy information products containing their own identifying information directly from look-up services which have less stringent access requirements. Yet, even if consumers determined that information products contained inaccuracies about them, there currently is no mechanism for correcting errors. Moreover, correcting the error in one database may not solve the problem, as misinformation tends to resurface in the same database,[173] or show up later in others.

Although neither workshop participants nor commenters identified concrete evidence of harm linked directly to inaccurate records offered by look-up services, this can be explained by factors other than the absence of such harm. Most consumers have no way of knowing that adverse decisions affecting them are made based on inaccuracies obtained through the look-up services. First, most consumers are unaware of the existence of look-up services. Second, most look-up services do not maintain audit trails of their customers' uses, and, therefore, cannot determine whether an entity who has made a decision affecting a consumer had in fact used a look-up service to access that consumer's files. Finally, except when users make decisions to deny credit, insurance, or employment based on a consumer report (containing, *e.g.*, credit history, financial status, and employment background information) obtained from the look-up

services, the users have no obligation to notify the data subject that an adverse decision was based on information obtained through a look-up service.[174]

C. Risks Associated With Unlawful Uses

Increasing access to personal identifying information also poses troubling risks of unlawful uses. Whether initially obtained by an unscrupulous employee, a scam artist able to side-step access restrictions, a computer hacker,[175] or an Internet surfer, personal identifying information in the wrong hands can have severe repercussions.[176]

One risk is that certain users, although they have an apparently legitimate purpose for accessing information through the service, may exploit their access and use the information for illegal purposes, like fraud. Responsible individual reference services do employ security measures to limit wrongful use, for example by having their customers require employees to sign non-disclosure agreements. Yet, reported incidents about employees in other industries who have access to personal identifying information demonstrate that such measures do not always work. Employees sometimes sell information they obtain from their employers' databases, or exploit it themselves. In one highly-publicized incident, a prison inmate (and convicted rapist), who, along with other inmates, was retained by an information vendor as a data processor, had legitimate access to a database containing personal information, and then used the information to compose and send a personalized, threatening letter to an Ohio grandmother.[177] Additionally, a used car salesman was caught using information in a consumer's credit report for illicit purposes.[178] Similarly, according to the Secret Service, perpetrators of fraud are increasingly buying consumer information from corrupt bank employees.[179]

Wrongful access by hackers is another risk. In response, certain companies have implemented firewalls.[180] Computers, however, are notoriously insecure.[181] Hackers can break into even the most impervious databases searching for information.[182] Three German hackers who successfully penetrated the firewall of an Internet service provider siphoned its entire list of 11,000 customers, including detailed credit applications, and threatened to post it on the Internet.[183] A California man downloaded 100,000 credit card numbers by tapping into the Web sites of online retailers.[184] According to the FBI, reports of wrongful access to information stored in computers have increased more than six-fold since 1991.[185] Furthermore, at the end of the third quarter of 1997, the FBI had 392 pending cases of wrongful access, compared to 99 at the end of 1995.[186] Given the demonstrated insecurity of computers, these risks may persist regardless of any regulation.

Commenters and workshop participants are concerned that identity theft and credit card fraud will increase with the growth of the individual reference services industry.[187] The harm caused by identity theft is not merely the financial exposure of victims,[188] banks, and lending institutions. It sometimes takes years of time and frustration for victims to re-establish their own identities, and their harm is difficult to quantify.[189]

Identity thieves have historically used low-tech means to accomplish their crimes such as stealing pre-approved credit applications from mailboxes or obtaining credit card receipts from trash dumpsters.[190] A recent case brought by the United States Secret Service, however, demonstrates how computer-savvy identity thieves may exploit information available over the Internet. The defendants, a Maryland couple who were arrested last June and who pled guilty in September, admitted not only to stealing the identities of

hundreds of individuals, but also to routinely using Internet databases (accessed at a local community college) to select their victims.[191] According to the Delaware detective who investigated the case, the couple sought affluent individuals who lived in the South, where states typically use Social Security numbers as drivers' license identification numbers.[192] The couple obtained official birth certificates, driver's licenses, credit cards, and bank accounts, and ran up debt exceeding $100,000 under their assumed identities.[193] It is unclear, however, whether they relied on look-up services, or simply gathered information from published materials generally available on the Internet.[194]

Individual reference services potentially could facilitate identity theft and credit card fraud in several ways. First, if the perpetrator has already identified the victim, she could use those services that display Social Security numbers to obtain the victim's Social Security number and other necessary identifying information. As the Court of Appeals for the Fourth Circuit has observed, "[s]uccinctly stated, the harm that can be inflicted from the disclosure of a Social Security Number to an unscrupulous individual is alarming and potentially financially ruinous."[195] Many services that do not display Social Security numbers do allow searches by Social Security number, so that when a user enters a Social Security number, the service retrieves the record of the individual associated with that number, including name, address, and date of birth.[196] Anyone willing to spend some time and money, therefore, could run searches with strings of nine digits (fabricated Social Security numbers) until she finds an identity worth impersonating.[197] Once an identity thief has selected the name and Social Security number of a potential victim, gaining access to an individual reference service would afford her additional lucrative information, such as the assets and professional licenses associated with that identity. This information would enable the identity thief to select identities with potentially high credit limits.

Industry representatives emphasize that the Federal Reserve Board (hereinafter "FRB") found little hard evidence linking identity theft to the look-up services.[198] However, the FRB concluded that "fraud related to identity theft appears to be a growing risk for consumers and financial institutions, and the relatively easy access to personal information may expand the risk."[199] As discussed above, the lack of concrete evidence may be due to the fact that look-up services often do not keep records of who has accessed which information products. Therefore, it would be difficult, if not impossible, to link a case of identity theft to an individual reference service, unless perpetrators admit to their source for information. It is difficult to know whether the lack of audit trails is preventing the development of evidence linking the look-up services to identity theft. On the other hand, evidence does indicate that databases can be used to *reduce* the risk of identity theft and credit card fraud, because access to credit header information and other verification tools enables database users to detect attempts at wrongful use of Social Security numbers.[200]

Physical harm perpetrated by violent stalkers and domestic abusers is an additional troubling risk associated with look-up services.[201] Regardless of their efforts to conceal their whereabouts, potential victims who provide their new address to credit grantors -- who in turn report it to the credit reporting bureaus, who in turn sell it to the individual reference services -- can be easily found.[202] According to one law enforcement organization, accessing government records is the most common way that rapists locate their victims,[203] and perpetrators of domestic violence can easily find relatives who have relocated in an effort to escape.[204] Individual reference services make government records easy to access. This fact is particularly unnerving, given that many of these services provide location information about children.[205] The infamous murder of actress Rebecca Schaeffer, whose predator tracked her down by having a private investigator access her DMV records from a computerized database, demonstrates the potential harm.[206] Additionally, many individuals, because of their occupations, are vulnerable to unwanted intrusions at home. Such individuals include: police officers and other employees in the law enforcement and justice

systems; teachers; doctors and other health professionals; psychological counselors; social workers; and employees of "unpopular" government agencies.[207] In fact, access to public records information has enabled criminals to track down the residences of their arresting officers.[208] Although the availability of public records information from government custodians already poses risks, the look-up services greatly facilitate access to the public records, and thereby substantially increase those risks.

V

Controls

The commenters and workshop participants recommended various controls that might address the concerns raised by the existence of the look-up services. These controls include: (1) limiting the availability of sensitive identifying information; (2) monitoring how customers use information and maintaining audit trails; (3) allowing consumers to access information maintained about them and to dispute inaccuracies; (4) providing consumers with control over how information about them is used; and (5) educating consumers about the industry, its information practices, and related privacy issues, and educating business about consumer privacy interests. As discussed above, certain members of the industry have implemented some of these controls, and others have not.

A. Limiting the Availability of Sensitive Information

1. Limiting Access to Information Obtained Through Individual Reference Services

Several participants at the June 10, 1997 Workshop and commenters (responding to the Commission's *Federal Register* notice) urge that individual reference services take precautions to limit access to personal identifying information and to prevent its misuse.[209] A core element of fair information practices identified through government efforts is that parties who create, maintain, or disseminate personal identifying information must prevent its misuse by others.[210] Completely barring the availability of all information could eliminate potential benefits, while making information available to everyone without restriction could maximize the potential risks. Accordingly, one approach is to limit access to customers who can be trusted to use it for specified purposes. Given that certain categories of information,[211] and certain types of users, pose more of a threat to consumers, access limitations could be a function of both the category of information sought and the type of user.

Who should have access to what types of information? One potential means to limit access to sensitive information, like Social Security number and birth date, would be to determine on a case-by-case basis whether a particular user has a legitimate purpose to obtain such information.[212] One Workshop participant advocated that such restrictions require that look-up services, before granting

access, verify that the user is who she says she is, and that she is a legitimate entity with a legitimate purpose.[213]

Other approaches were also posited. Allowing only law enforcement officials to access information through individual reference services is one alternative approach. However, such a limitation would eliminate not only private sector benefits not directly connected to law enforcement, but perhaps even benefits connected to law enforcement as well. For example, government child support enforcement, and other law enforcement, agencies are burdened with an extreme backlog of cases and often cannot pursue all worthy cases. As a result, several private agencies assert that they help public agencies carry out their law enforcement missions.[214]

Another possibility would be to allow access for only law enforcement-related purposes, and allow the look-up services to be used by public and private agencies for child support enforcement, finding missing children, and other similar ends. Private entities are concerned about this approach, as well. First, it would exclude journalistic uses[215] and important industry uses, like fraud prevention.[216] Second, one panelist suggested that her child support enforcement agency and other public interest groups enjoy free or discounted services.[217] As the services would not be able to make the same profits if they restricted the access of users who would otherwise pay the full cost, the participant was concerned that such restrictions could so severely impair the companies' profit incentives that they would no longer provide the services,[218] or no longer provide free or discounted services. Yet another suggested approach would be to limit access to regulated or licensed entities, such as lawyers and private investigators, in addition to law enforcement agents.[219] Misuse of information by these parties would have repercussions, such as license revocation.[220] However, not all users who have potentially beneficial purposes for accessing information are regulated entities. This approach would exclude access by private investigators in several states without licensing requirements, journalists, and much of private industry.

2. Minimizing Extraneous Sensitive Identifying Information in Public Records

The increasing availability of public records facilitates easy access to sensitive identifying information which, as described above, could have harmful consequences. Another possible control, therefore, would be to minimize the sensitive identifying information that government entities gather and/or make publicly available.[221] In general, access to public records furthers important societal objectives. For example, wide dissemination of title information in land registers advances the public notification purposes of land recording statutes.[222] Court records can inform the public about questionable prosecutorial policies, low conviction rates, and fraudulent schemes requiring legislative attention.[223] The availability of professional license information enables consumers to avoid being harmed by the services of unqualified professionals.[224] It is possible, however, that the collection and/or dissemination of sensitive information, like Social Security number, mother's maiden name, and date of birth, does not directly advance the purpose underlying the requirement of a given public record.[225] Limiting the availability of public records once information has been collected by government agencies may raise some concerns; *e.g.*, it could erode the public's right to know,[226] and impose costs on public records custodians.[227] However, continuing to make available information that advances a government agency's intended purpose while minimizing the extraneous, sensitive information could help reduce potential harm

3. Heightening Security Measures

Commenters expressed concern about protecting the information from *unauthorized* access.[228] Accordingly, they recommended that services minimize risks by heightening security controls. Commenters urged individual reference services to employ technological protections, such as firewalls and encryption, as well as measures to prevent unauthorized disclosures by employees.[229]

B. Monitoring Use and Maintaining Audit Trails

Two additional controls related to access restrictions include monitoring use and maintaining audit trails. Access restrictions based on purpose are meaningful only if controls are in place to ensure that users who obtain information for a stated legitimate purpose actually use information consistently with that purpose.[230] Monitoring the use of information would accomplish this end. Similarly, the maintenance of audit trails -- records of which users have accessed what information -- may enable a company to link misuse to a particular user, and thereby identify instances where users asserted a legitimate purpose but used information wrongfully.[231] Without audit trails indicating to whom and for what purpose information has been sold, some maintain that consumers have no recourse upon being harmed by misuse of their information.[232] Audit trails also may be important at the front end, as a deterrent: if potential abusers of information knew that the information they obtain could be traced back to them, they arguably would be less likely to misuse it.

Although certain look-up services do maintain audit trails, according to industry members, they are problematic for two reasons: (1) maintaining records of every search run by every customer would be unreasonably costly and (2) because records of what information an attorney accessed could be discoverable in a lawsuit, companies that maintain audit trails might lose attorney clients. Furthermore, audit trails are not completely effective in tracking misuse of information because a wronged consumer or law enforcement entity investigating misuse would first have to know which look-up services were accessed in order to determine which service's audit trails to examine.[233] However, if an entity did know which look-up services were accessed, or if the entity simply inquired with several of the look-up services, audit trails would increase the likelihood that a wrongdoer would be tracked down.

C. Allowing Consumers to Access Their Own Information and Dispute Inaccuracies

Many argue that, at a minimum, consumers must have reasonable access to information maintained about them by individual reference services.[234] Without access to their own records, consumers have no way to know whether information that is disseminated about them is accurate. Consumer access requirements have also surfaced as an integral element of fair information practices in several similar contexts.[235] For example, consumer access has proven to be critical in the context of credit reporting. Credit reports are subject to federal legislation which requires, among other things, that consumer reporting agencies (*e.g.*, credit bureaus) provide consumers with a copy of their credit report and follow reasonable

procedures to assure maximum possible accuracy of information contained in the report. [236] The justification underlying this requirement is that information contained in the credit report may be used to make decisions that adversely affect consumers. [237] Thus, consumers have the right to see what information is in their credit file.

The individual reference services serve their customers -- entities who use information to take actions impacting data subjects -- and not the data subjects themselves. While there is an obvious incentive to give their customers accurate information, the individual reference services have less incentive to address concerns of data subjects. [238] The adverse effects on data subjects caused by inaccuracies in records maintained about them, including personal information gleaned from non-public sources or outdated, incomplete, or mismatched public records, can be much more severe than their impact on customers. [239] An information industry association argues that it is too burdensome to provide data subjects with access to their records. [240] However, the cost of providing consumers access could be passed on in the form of fees. Proponents of consumer access do not oppose the imposition of such fees, so long as they are reasonable. [241]

Providing consumers with access to records held about them is a first step toward ensuring that data is accurate. This access is meaningful only with a method in place that allows consumers to correct inaccuracies. To help ensure that records maintained about individuals are as accurate as possible, look-up services should also obtain information only from reputable sources and must implement a system that enables individuals to dispute and correct inaccuracies. [242] The industry maintains that look-up services are not able to change or delete information that is in a public record and therefore they cannot change or delete data they maintain that originated from public records. [243] This position assumes that public records information maintained by the look-up services mirrors the original public records, and overlooks the fact that public records information may not be accurate once it is transferred from the custodian of public records and merged with other data. It may not be current. It may reflect transcription or transmission errors. Or, it may have been erroneously linked with the records of a different individual having the same or similar name.

D. Providing Consumers with the Ability to Opt Out or Opt In

Some privacy and consumer advocates assert that consumers should have the ability to make an informed choice as to whether to permit individual reference services to make their personal identifying information available. [244] This choice (or "consumer control") would necessarily take the form of either "opt in," requiring the look-up services to affirmatively obtain an individual's permission before making information about them available, or "opt out," permitting the look-up services to disseminate information about a particular consumer until the consumer instructs them otherwise. Only a select few individual reference services allow consumers to opt out of one or more of their databases. [245] Proponents of consumer control note that an opt out option is meaningless if consumers are unaware that a database exists. [246] Accordingly, some suggest that either an opt in option should be mandated, [247] or consumers should have the ability to opt out only once, through a universal system that affects all services. [248] Not all proponents of consumer control assert that the control should extend to public records; some support making public records information available regardless of consumer consent as long as the information is made available for free, and there is no legitimate economic incentive to exploit it. [249]

Although giving consumers control over the secondary use of their personal identifying information is an accepted fair information practice in several contexts,[250] here this approach is not without significant costs. In addition to individuals simply concerned about their privacy, those who would most likely choose to have their records excluded from the look-up services are those whom law enforcement agencies and other societally beneficial groups most want to find.[251] Users of the look-up services assert that the more complete the databases, the more useful they are in allowing such users to achieve their ends,[252] and that giving individuals complete control over information in this area likely would severely diminish the important societal benefits these services confer.[253] One possible means of giving individuals control over their information without eliminating the industry's benefits would be to allow individuals to opt out of some, but not all, uses of their information.

E. Educating Consumers and Business

Many consumer and privacy advocates assert that consumers must be made aware of the existence of the individual reference services industry and of the available methods to control the use of their personal information (such as their ability to opt out of certain databases).[254] The concern that individuals should be informed about personal information record keeping systems has been repeatedly identified as an element necessary to protect consumer information privacy interests.[255] Several Workshop participants and commenters, including industry representatives, acknowledged that education about this industry is necessary.[256] One consumer advocate stressed that consumers need to learn about the risks of misuse of their personal information and not just the benefits of data collection and availability;[257] another noted that companies do not have an incentive to educate consumers about threats to their privacy.[258] Furthermore, privacy advocates argued that the industry should learn about the role that consumer privacy should play.[259]

VI

IRSG Proposal

In response to the Commission's announcement of this study, members of the individual reference services industry, including information suppliers and direct providers of commercial services (referring to themselves as the "Individual Reference Services Group" or "IRSG Group"), announced their intention to draft self-regulatory principles. Since the industry group's announcement, Commission staff has monitored and encouraged its progress.[260] Fourteen industry members have agreed to follow these self-regulatory principles (hereinafter the "IRSG Principles" or "Principles"). The signatories include companies that directly offer individual reference services, information vendors, and three national credit agencies.[261] The Principles set forth controls which address most concerns raised by the industry's dissemination of non-public information, defined as "information about an individual that is of a private nature and neither available to the general public nor obtained from a public record."[262]

The Principles do not address the practices of online white-pages directory services, because the latter are not "commercial services" as contemplated by the Principles. However, this exclusion does not appear problematic. The majority of Internet white-pages services have already addressed consumer concerns by not displaying unlisted directory information, by permitting consumers to opt out, and by not allowing reverse address and telephone searches.[263] Furthermore, these services make available only directory information, not more sensitive identifying information such as Social Security number and date of birth.

A. The IRSG Principles

1. Restrictions on the Availability of Non-Public Information

The Principles impose restrictions on access to information obtained from non-public sources, or "non-public information" (*e.g.*, mother's maiden name and Social Security number obtained from "credit headers").[264] To the extent information obtained from a non-public source is publicly available, such as a home address that appears in a "credit header" but also is listed in the phone book, that information is *not* treated as "non-public." The Principles completely bar look-up services from making available certain non-public information, namely information gathered for marketing purposes.[265] Otherwise, the nature of information provided by an individual reference service and corresponding controls vary according to the category of customer. There are three categories of customers: "qualified subscribers," "professional and

commercial users," and the general public. In general, customers that have less restricted access to non-public information ("qualified subscribers" and "professional and commercial users") are subject to greater controls. Conversely, the general public has more restricted access to non-public information and is subject to fewer controls. The particular categories of customers, the information available to them, and the corresponding controls are described below.

The Principles allow unrestricted distribution of certain non-public information only to "qualified subscribers." An entity can access services as a "qualified subscriber" only after: (1) the service conducts a reasonable review of the subscriber and its intended uses of the information; (2) the service determines that the intended uses are "appropriate;"[266] (3) the entity agrees to limit its use and redissemination of such information to such "appropriate" uses; and (4) the entity agrees to terms and conditions consistent with the Principles.[267] Depending on the particular signatory, "qualified subscribers" might include law enforcement agencies and private investigators, and "appropriate" uses might include locating criminal suspects or the searching for missing children.[268]

The distribution of non-public information is more restricted for the category of "professional and commercial users." This category includes entities falling somewhere between qualified subscribers, who have a legitimate need for sensitive information, and the general public. "Professional and commercial users" can access certain non-public information if they use it in the normal course and scope of their business and profession, and if the use is appropriate for such activities. While they do not undergo the strict qualification process imposed on subscribers in the first category, they do not enjoy access to the same non-public information. They can access only truncated Social Security numbers (meaning a portion of the Social Security number has been replaced by "X"s), and month and year of birth (not full date of birth), and cannot access mother's maiden name or information that reflects credit history, financial history, or medical records. Furthermore, users in this category may access non-public information about children only for purposes of finding missing children.[269] At the same time, because members of this category are professional users whose professional use is linked to the need to access information, they can access more information than can the general public. Before granting access to non-public information to a "professional or commercial user," the services must: (1) establish that the user is a professional or commercial entity; (2) require the user to agree to terms and conditions consistent with the Principles; and (3) require the user to use the information to advance its business or professional purpose, and to limit any redissemination of such information to such uses, in accordance with the Principles.[270] Depending on the company, examples of "professional and commercial users" might include lawyers seeking to locate potential witnesses, marketers assuring the accuracy of their potential customer lists, and banks seeking to detect fraud.

The third category, "general distribution," includes the general public. The Principles prohibit individual reference services from distributing to the general public certain non-public information such as Social Security number, mother's maiden name, birth date, credit history, financial history, medical records, or similar information, or any information about children. They also prohibit making available both unlisted telephone numbers obtained from sources other than public records and unlisted addresses obtained from the telephone company. However, services may make available unlisted addresses if they are obtained from sources other than the telephone company, such as the gas company. Furthermore, look-up services may not allow the general public to run searches using Social Security number as a search term.[271]

To protect the security of sensitive information, look-up services are required to maintain facilities and systems to protect information from unauthorized access. In addition to physical and electronic security, look-up services must require employees and contractors to sign confidentiality agreements and to be subject to supervision. The Principles require services to conduct system reviews at appropriate intervals to ensure that employees are complying with policies.[272]

2. Monitoring Use and Maintaining Audit Trails

The Principles require the look-up services to take reasonable steps to protect against the misuse of non-public information.[273] Each service must make available upon request an explanation of the uses of its non-public information it deems appropriate for "qualified subscribers," as well as an explanation of the types of "qualified subscribers" that can access such information.[274] The services must take reasonable steps to remedy abuses of the information by "qualified subscribers" and "professional and commercial users,"[275] and must employ reasonable measures to ensure that the information is used appropriately.[276] Furthermore, individual reference services must maintain, for three years after termination of each subscriber's relationship with the individual reference service, a record of the identity of each subscriber in these two categories, the types of uses employed by the subscriber, and the terms and conditions agreed to by the subscriber.[277] The look-up services are not required to maintain records of what information their users accessed.

3. Consumers' Access to Personal Information and Methods to Ensure Information Accuracy

Upon an individual's request, the Principles require a look-up service to provide copies of *non-public* information in its products and services that specifically identifies the individual.[278] The Principles do not compel the companies to provide individuals with copies of the *public* information that identifies them (*e.g.*, real estate records, court records, licenses, and other publicly available information). Rather, the Principles provide that each signatory shall inform individuals about the *nature* of public record and publicly available information that it makes available and the general sources of such information;[279] *i.e.*, not specific sources, but rather the entire universe of public records sources from which they create their databases.[280] As a result, under the Principles, individuals have no way of seeing files about them that reflect compiled public records information.

The Principles incorporate several measures to ensure that information products are accurate. First, identifying information may be acquired only from known, reputable sources whose data collection practices and policies are understood.[281] The services must take reasonable steps to help ensure the accuracy of the information.[282] Upon being informed of an inaccuracy by an individual, a service must either correct the inaccuracy or inform the individual of the source of the information. It must also tell the individual where a request for correction may be directed, if that information is reasonably available.[283] The Principles do not compel look-up services to correct inaccuracies reported by an individual about public record or publicly available information maintained by the services about that individual.

4. Ability to Opt Out

The Principles provide individuals with the ability to opt out of only "general distribution" of their non-public information.[284] Individuals may not opt out of distribution to "qualified subscribers" or to "professional and commercial users." Furthermore, signatories may not make available "unlisted" telephone numbers or addresses obtained from a telephone company.[285] If an individual has not opted out of a service's general distribution, however, the service is permitted to make available that individual's "unlisted" name and address if it obtains the information from sources other than the telephone company. Upon request, the signatories must also inform individuals of any other choices available to limit dissemination of their information.[286]

5. Consumer Education and Openness

The Principles require the individual reference services to educate users and the public about privacy issues associated with their services, about the types of services they offer, and about the Principles.[287] In addition, each service must make available a privacy policy statement that describes what information it has from what types of sources, how it is collected, the type of entities to whom it may be disclosed and the type of uses to which it is put.[288] The services must also notify consumers about their practices through Web sites, advertisements, or company- or industry-initiated educational efforts.[289]

6. Compliance Assurance

The enforcement program has two prongs. First, signatories' practices will be subject to a review by a "reasonably qualified independent professional service." That entity will determine whether a signatory is in compliance with the Principles, using criteria based upon the Principles.[290] The summary of the annual review will be made public. Second, the Principles provide that signatories who are information suppliers may not sell information to look-up services that do not comply with the Principles.

B. Analysis of IRSG Proposal

The record reflects opposing views as to the very notion of self-regulation. Supporters of self-regulation believe that industry should be given the opportunity to regulate its own practices, and that government action should be taken only if this approach proves ineffective.[291] Critics point to one central weakness with this approach: the lack of either incentive or mechanism for enforcement.[292] They also highlight several difficulties, such as influencing industry members who do not adhere to self-regulatory schemes,[293] sustaining a self-regulatory program once public attention wanes,[294] and addressing nuanced privacy-related issues.[295]

In determining whether the IRSG Principles offer a viable self-regulatory program, the Commission has assessed the extent to which the Principles can effectively implement controls similar to those set forth in Section IV above. These controls include: (1) limiting the availability of sensitive information; (2) monitoring use and maintaining audit trails; (3) allowing individuals to access records maintained about them and dispute inaccuracies; (4) giving individuals control over their information (provided this would not impede important public interests); and (5) educating consumers and business about information practices and privacy issues. Even if such controls are set forth in principle, the Commission believes that

they are not meaningful without an effective mechanism to assure compliance and to influence the practices of the entire industry.

The Principles address the first control, limiting the availability of sensitive information, through the three-tiered customer category scheme. These access restrictions not only prohibit signatories from making available to the general public Social Security numbers, full dates of birth, and information about children (which are obtained from non-public sources and not otherwise publicly available), but also limit the extent to which established, professional entities can obtain this information. Furthermore, before signatories can provide unrestricted access to information, they must take measures to verify the identity of potential users and establish the legitimacy of their purposes.

The Principles address the second control, monitoring use and maintaining audit trails, in part by requiring that signatories take measures to protect against misuse of all non-public information. Signatories must ensure that the more potentially sensitive information, which is available only to "qualified subscribers" and "professional and commercial users," is used properly; if it is not being used properly, they must remedy misuses. Moreover, signatories have to keep track of the identities as well as the *types* of information (but not the actual information) accessed by these two categories of users.

With regard to the third control, individuals' access to their own information, signatories must allow individuals to access *non-public* records maintained about them and dispute inaccuracies. As to the fourth safeguard, consumer control, the Principles allow individuals to opt out of the general distribution of their *non-public* information, but not out of distribution to qualified, professional, or commercial users. Finally, the Principles include the fifth control, education, by requiring signatories to notify consumers as to their information practices and to educate them about privacy issues related to their industry.

Most important, the IRSG Principles show promise for success in a critical area: the framework should assure compliance by both signatories and other members of the industry. The signatories characterize themselves as the "vast majority" of the industry that supplies information to commercial users.[296] Thus, the vast majority of the industry has agreed to annual compliance reviews -- an innovative step for a self-regulatory program, particularly as applied to information practices. Publicizing the results of compliance reviews performed on signatories (and their customers) by third parties, coupled with potential liability under the FTC Act and similar state statutes for non-compliance, should assure the signatories' compliance.[297] In instances where non-signatories' practices are inconsistent with the Principles, they will likely be unable to obtain non-public information easily to redisseminate through their services. Major suppliers of non-public information to this industry -- and the only primary suppliers of credit header information -- have agreed to sell only to companies whose practices are consistent with the Principles. Therefore, the Principles can be expected to have a beneficial impact on the practices of even those entities who are not signatories.[298]

The IRSG Principles fail, however, to incorporate all the suggested controls, and therefore do not address important concerns that have been raised about the industry. First, they provide essentially no limitations on the availability or uses of public records and publicly available information.[299] Accordingly, they do not limit the potential harm that could stem from access to and exploitation of sensitive information in public records and publicly available information. Second, the Principles fail to require individual reference services to maintain audit trails of the precise records accessed by each user, an important mechanism for identifying when an apparently legitimate entity obtains and uses information illegitimately and possibly the only mechanism that can link harm to the look-up services.[300] Third and most notably, the

Principles fail to provide individuals with a means of accessing public records and other publicly available information maintained about them by individual reference services. The Commission is concerned that individuals have no way of discovering or correcting errors that may have occurred in the transcription, transmission, or compilation of this information.[301] Accordingly, the individuals cannot prevent, let alone identify, situations where that inaccurate information results in decisions which may adversely affect them. The Group is aware of this problem, and has stated that it will seriously consider conducting a study about the extent of relevant inaccuracies and related harm.[302]

Notwithstanding these shortcomings, the Principles have the potential to (1) curb misuse of non-public, personal identifying information; (2) address many of the relevant consumer information privacy concerns; and (3) significantly affect the practices of the entire individual reference service industry. The IRSG proposal is more comprehensive and far-reaching than any other voluntary, industry-wide program in the information sector. Members of the IRSG Group have made rapid and significant strides toward responding to consumers' concerns.